III Выводы

1. Актуальной задачей является разработка, производство и сертификация недорогих эффективных отечественных ГШ, реализующих пространственное и линейное зашумление опасных сигналов в электромагнитном и электрическом каналах утечки информации.
2. В рамках решения этой задачи в Национальном университете внутренних дел были разработаны и исследованы макеты ГШ радиодиапазона (0.05...1500 МГц) и СГШ (0.1...15 МГц).
3. Разработанные ГШ по базовым техническим характеристикам не уступают, а по ряду из них (диапазон защищаемых частот, массогабаритные показатели, цена) превосходят известные ГШ.
4. На основе энергетического критерия показано, что в общем случае ГШ радиодиапазона не обеспечивают подавление акустических радио закладок, но позволяют упростить (удешевить) процесс обнаружения мощных кварцованных РЗ.
5. Использование широкополосных ГШ радиодиапазона для активной защиты от РЗ дает положительный эффект только в ряде частных случаев:
   – наличия в составе РЗ радиоканала ДУ, приемное устройство которого будет подавлено маскирующей помехой ГШ;
   – пониженной до значений сотен мкВт…единиц мВт мощности излучений РЗ для повышения скрытности его работы;
   – наличия априорной информации о вероятной зоне технической разведки и выносе ГШ в сторону работающего с РЗ приемного устройства. Радиус зоны подавления может составлять от единиц до нескольких десятков метров.
6. В целях надежного блокирования электрического КУИ, образованного мощными кварцованными сетевыми закладными устройствами в условиях априорной неопределенности о диапазоне их работы и виде модуляции сигналов, целесообразно комплексирование активного и пассивного методов защиты. Оно может быть реализовано на основе сопряжения в едином устройстве сетевых фильтра и ГШ, требования к базовым характеристикам которых (коэффициенту подавления фильтра, спектральной плотности мощности шума) могут быть снижены.

Литература: 1. Захист інформації. Технічний захист інформації. Основні положення. ДСТУ 3396.0-96. 2. Энциклопедия промышленного шпионажа / Под общ. ред. Е. В. Куренкова – С.-Петербург: ООО "Изд-во Полигон", 1999. – 512 с. 3. Хорев А. А. Защита информации от утечки по техническим каналам. Часть 1. Технические каналы утечки информации. Уч. пособ. М.: ГТК России, 1998. – 320 с. 4. Емельянов С. Л., Логвиненко Н. Ф., Марков С. И., Носов В. В. Проблемные аспекты разработки, производства и применения отечественных генераторов шума в системах защиты информации // Сбірник матеріалів II НТК "Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні". Київ, 2000. С. 159 – 162. 5. Ю. Зиньковский, В. Клименко. Задачи электромагнитной технической защиты основных информационно-вычислительных средств // Там же. С. 87 – 92. 6. В. Первой, В. Швайченко. Эффективность помехоподавляющих защитных фильтров в двух и трёхпроводных однофазных электрических сетях // Там же. С. 184 – 187. 7. Каталог МАСКОМ. Специальная техника защиты информации, М., 1998. С. 9. 8. Вакин С. А., Шустов Л. Н. Основы радиопротиводействия и радиотехнической разведки. М.: Изд-во "Сов. Радио". 1968. - 448 с. 9. Емельянов С. Л., Логвиненко Н. Ф., Марков С. И., Носов В. В. Технические методы защиты каналов утечки информации по электросети // Бизнес и безопасность, № 2, 2000. С. 8 – 9.

УДК 004.056.5

ПРИМЕНЕНИЕ ФОРМАЛЬНЫХ МОДЕЛЕЙ БЕЗОПАСНОСТИ ДЛЯ АНАЛИЗА ЗАЩИЩЕННОСТИ СИСТЕМ ОТ НЕСАНКЦИОНИРОВАННОГО УДАЛЕННОГО АДМИНИСТРИРОВАНИЯ

Денис Кудин, Владислав Корольков
ООО «Центр информационной безопасности», Запорожский государственный

технический университет

Аннотация: **Рассматриваются подходы к организации подсистемы защиты в операционных системах, описываются классические формальные модели политики безопасности и оценивается возможность их применения для анализа защищенности систем от несанкционированного удаленного администрирования.**

Summary: **The ways of building the security subsystem in operating systems, classic formal security policy models and their application for evaluation of protection from unauthorized remote administration are considered in this article.**

Ключевые слова: **Операционная система, удаленное администрирование, политика безопасности, модель безопасности, подсистема защиты.**

Технологии удаленного администрирования используются для доступа и управления ресурсами информационных систем из внешней среды. В последние годы данные технологии приобретают все большую актуальность благодаря широкому распространению различных информационных систем во всех сферах общественной жизни. При этом неотъемлемой частью являются вопросы безопасности объектов информационной деятельности, т. к. несанкционированный доступ к критичной информации, и тем более ее модификация, может нарушить работоспособность системы и объекта в целом, создать угрозу безопасности общества и т. д.

Методы удаленного администрирования в первую очередь опираются на возможности и свойства операционных систем (ОС). В большинстве современных ОС средства удаленного администрирования встроены в ядро системы или реализуются с помощью специального программного обеспечения. Без исследования таких средств и свойств ОС невозможно разрабатывать защищенные компьютерные системы на их основе, поскольку, как известно, безопасность всей системы оценивается как защищенность самого слабого ее звена. В данном случае слабым звеном являются технологии, позволяющие злоумышленнику с другого континента несанкционированно управлять ресурсами удаленных автоматизированных систем.

В реальном мире существует множество технологий для вторжения в систему, включая использование скрытых каналов получения информации, недокументированных возможностей операционной системы, создание новых каналов получения информации с помощью программных закладок, применение легальных и нелегальных программ удаленного доступа и администрирования, заражение системы программными вирусами, хищение носителей информации, нарушение физической защиты и др. Эти процессы очень сложны для моделирования, и при их формальном описании невозможно учесть все внешние и внутренние факторы, влияющие на их протекание и взаимодействие. Поэтому широко используется практика упрощения системы и введения обобщенных критериев оценки ее безопасности, с использованием которых разрабатываются специализированные формальные модели безопасности исследуемых систем.

Рассмотрим особенности классических формальных моделей безопасности операционных систем с точки зрения их применимости для анализа защиты от несанкционированного удаленного администрирования как одной из угроз безопасности автоматизированных систем. Но прежде, остановимся на существующих подходах к организации подсистемы защиты ОС.

Согласно [1], защищенной является система, способная обеспечить защиту обрабатываемой информации от определенных угроз. Угрозы безопасности ОС существенно зависят от условий эксплуатации системы, от того, какая информация хранится и обрабатывается в системе, и т.д. Например, если ОС используется главным образом для организации электронного документооборота, наиболее опасны угрозы, связанные с несанкционированным доступом к файлам. Если же ОС используется как платформа для провайдера услуг Интернет, то очень опасны атаки на ее сетевое программное обеспечение.

Существует два основных подхода к созданию защищенных операционных систем – частичный и комплексный. При частичном подходе сначала организуется защита от одной угрозы, затем от другой и т.д. Примером частичного подхода может служить ситуация, когда за основу берется незащищенная операционная система, затем на нее устанавливается антивирусный пакет, система шифрования, система регистрации действий пользователей и т. д. Основной недостаток такого подхода очевиден – подсистема защиты операционной системы представляет собой набор разрозненных программных продуктов разных производителей, работающих независимо друг от друга без возможности налаживания их взаимодействия.

При комплексном подходе к организации безопасности системы защитные функции вносятся в ОС на этапе планирования ее архитектуры и являются неотъемлемой ее частью. Отдельные элементы подсистемы защиты, созданной на основе комплексного подхода, тесно взаимодействуют друг с другом при решении различных задач, связанных с организацией защиты информации. Кроме того, такая подсистема защиты может быть устроена так, что при фатальных сбоях в функционировании ее ключевых элементов она

ISBN 966-622-022-9
Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2, 2001 р.

вызывает крах всей операционной системы, что не позволяет злоумышленнику отключать ее защитные функции [2].

Опишем основные функции, выполняемые подсистемой защиты ОС.

– **разграничение доступа**: каждый пользователь системы имеет доступ только к тем объектам ОС, к которым ему предоставлен доступ в соответствии с текущей политикой безопасности;

– **идентификация и аутентификация**: ни один пользователь не может начать работу с ОС, не идентифицировав себя и не предоставив системе информацию аутентификации, подтверждающую, что пользователь действительно является тем, за кого он себя выдает;

– **аудит**: ОС регистрирует в специальном журнале регистрации события, потенциально опасные для обеспечения безопасной работы системы;

– **управление политикой безопасности**: политика безопасности должна постоянно поддерживаться в адекватном состоянии, т. е. должна реагировать на изменение условий функционирования ОС, требований к защите информации, хранимой и обрабатываемой в системе и т. д.

– **криптографические функции**: в ОС шифрование производится при хранении и передаче по каналам связи отдельных файлов и различных данных, критичных для безопасности системы;

– **сетевые функции**.

Современные ОС работают, как правило, не изолированно, а в составе локальных и/или глобальных компьютерных сетей. ОС компьютеров, входящих в одну сеть, взаимодействуют между собой для решения различных задач, в том числе и задач, имеющих прямое отношение к защите информации. В данную категорию входят, в частности, механизмы удаленного администрирования ОС.

Подсистема защиты практически никогда не представляет собой единый программный модуль. Как правило, каждая из перечисленных функций подсистемы защиты решается одним или несколькими программными модулями. Некоторые функции встраиваются непосредственно в ядро ОС. Тем не менее, должен существовать четко определенный интерфейс между различными модулями подсистемы защиты, используемый при их взаимодействии для решения общих задач.

Организация эффективной и надежной защиты ОС невозможна с помощью одних только программно-аппаратных средств. Эти средства должны обязательно дополняться административными мерами защиты, среди которых:

– постоянный контроль корректности функционирования операционной системы, особенно ее подсистемы защиты; такой контроль наиболее удобно организовать, если ОС поддерживает механизм регистрации событий; в этом случае ОС автоматически регистрирует в одном или нескольких журналах регистрации все события системы, заданные администратором;

– организация и поддержание политики безопасности, которая должна постоянно корректироваться, оперативно реагируя на изменения в конфигурации ОС, установку, удаление и изменение конфигурации прикладных программных продуктов и расширений ОС, попытки злоумышленников преодолеть защиту ОС и др.;

– инструктирование пользователей о необходимости соблюдения мер безопасности при работе с ОС и контроль над соблюдением этих мер;

– регулярное создание и обновление резервных копий программ и данных ОС;

– постоянный контроль изменений в конфигурационных данных и политике безопасности ОС.

Неотъемлемую роль в организации защиты ОС играет политика безопасности. При этом, основным инструментом доказательства соответствия системы защиты заданной политике безопасности являются формальные модели защиты.

В данных моделях, основанных на декомпозиции автоматизированной системы обработки информации на субъекты и объекты, ставятся и исследуются вопросы взаимодействия элементов системы с заданными свойствами. Целью анализа и последующей реализации модели является именно достижение таких свойств системы, как конфиденциальность и доступность [3]. Например, описывается дискреционный механизм безопасности, разделяющий доступ поименованных субъектов к поименованным объектам или полномочное управление доступом, моделирующее систему категорий и грифов доступа. Кроме того, результаты анализа формальных моделей позволяют систематизировать и направлять научные исследования по вопросам анализа и построения защищенных автоматизированных систем.

Рассмотрим фундаментальные модели безопасности, такие как Take-Grant, HRU и Bell-laPadula.

Модель распространения прав доступа Take-Grant основана на существенном упрощении реальной операционной системы с абстрагированием всего, кроме взаимосвязей между различными процессами или пользователями в системе, и моделированием динамических изменений параметров доступа, осуществляемым с помощью набора правил преобразования направленного графа, который отображает

данные взаимосвязи. Модель Take-Grant используется для анализа систем дискреционного разграничения доступа, в первую очередь для анализа путей распространения прав доступа в таких системах. Цель модели – дать ответ на вопрос о возможности получения прав доступа субъектом системы на объект в состоянии, описываемом графом доступов. Существует две разновидности модели Take-Grant – классическая и расширенная.

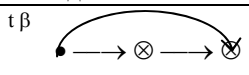
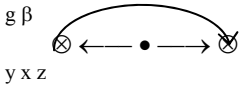
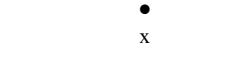
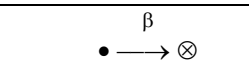
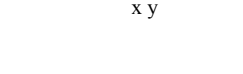
Введем следующие обозначения [3]:

O – множество объектов (например, файлов или сегментов памяти); $S \subseteq O$ – множество активных объектов – субъектов (например, пользователей или процессов); $R=\{r_1, r_2, \ldots, r_m\}\cup\{t,g\}$ – множество прав доступа, где t – право брать права доступа, g – право давать права доступа; G=(S, O, E) – конечный помеченный ориентированный граф без петель, представляющий текущие доступы в системе; множества S, O соответствуют вершинам графа, которые обозначим: ⊗ - объекты (элементы множества O\S); • - субъекты (элементы множества S); элементы множества $E \subseteq OxSxR$ представляют дуги графа, помеченные непустыми подмножествами из множества прав доступа R.

Состояние системы описывается ее графом доступов. Переход системы из состояния в состояние определяется операциями или правилами преобразования графа доступа. Преобразование графа G в граф G' в результате выполнения правила op обозначим через $G \vdash_{op} G'$, G'={S', O', E'}.

В классической модели Take-Grant существует четыре правила преобразования графа доступов, представленные в таблице 1.

Таблица 1

Исходное состояние (G)	Правило	Условия	Результат (G')
	**Брать** – take(α,x,y,z) субъект **x** берет у объекта **y** права $\alpha \subseteq \beta$ на объект **z**	$x \in S$ $y, z \in O$ $(x,y,t) \in E$ $(y,z,\beta) \in E$ $x \neq z$ $\alpha \subseteq \beta$ $G, \beta \subseteq R$	α  S'=S, O'=O, $E'=E \cup \{(x,z,\alpha)\}$
	**Давать** – grant(α,x,y,z) субъект **x** дает объекту **y** права $\alpha \subseteq \beta$ на объект **z**	$x \in S$ $y, z \in O$ $(x,y,g) \in E$ $(x,z,\beta) \in E$ $x \neq z$ $\alpha \subseteq \beta$ $G, \beta \subseteq R$	α  S'=S, O'=O, $E'=E \cup \{(y,z,\alpha)\}$
	**Создать** – create(β,x,y) субъект **x** создает новый β-доступный объект **y**	$x \in S$ $y \notin O$ $\beta \subseteq R$ $\beta \neq \varnothing$	β $O'=O \cup \{y\}$, $S'=S \cup \{y\}$, если у субъект, $E'=E \cup \{(x,y,\beta)\}$
	**Удалить** – remove(α,x,y) субъект **x** удаляет права доступа α на объект **y**	$x \in S$ $y \in O$ $(x,z,\beta) \in E$ $\alpha \subseteq \beta$ $G, \beta \subseteq R$	β \ α  S'=S, O'=O, $E'=E \setminus \{(x,y,\alpha)\}$

При санкционированном получении прав доступа не накладываются ограничения на взаимодействие субъектов системы, участвующих в этом процессе.

В том случае, когда предполагается возможность похищения прав доступа, предполагается, что передача прав доступа объекту осуществляется без содействия субъекта, изначально обладавшего передаваемыми правами. Пусть $x, y \in O$ – различные объекты графа доступа $G_0=(S_0, O_0, E_0)$, $\alpha \subseteq R$. Определим предикат «возможно похищение» (α, x, y, G_0), который будет истинным тогда и только тогда, когда

$$(x, y, \alpha) \notin E_0$$

ISBN 966-622-022-9
Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2, 2001 р.

и существуют графы

$$G_1=(S_1, O_1, E_1), \ldots, G_N=(S_N, O_N, E_N),$$

такие, что

$$G_0 \vdash_{op1} G_1 \vdash_{op2} \ldots \vdash_{opN} G_N \text{ и } (x, y, \alpha) \in E_N.$$

При этом, если

$$\exists (s, y, \alpha) \in E_0,$$

то

$$\forall z \in S_j, j=0, 1, \ldots, N$$

выполняется

$$opK \neq grant(\alpha, s, z, y), K=1, \ldots, N.$$

В расширенной модели Take-Grant рассматриваются пути и стоимости возникновения информационных потоков в системах с дискреционным разграничением доступа. В расширенной модели дополнительно рассматриваются два права доступа: на чтение и запись, а также дополнительные правила преобразования графов доступа. Эти правила служат для поиска путей возникновения возможных информационных потоков в системе, являются следствием уже имеющихся у объектов системы прав доступа и могут быть причиной возникновения информационного потока от одного объекта к другому без их непосредственного взаимодействия.

Универсальная модель для моделирования всех типов механизмов защиты, получившая название «**модель матрицы доступов HRU** (Harrison, Ruzzo, Ullman)» [4], или просто модель HRU, была представлена практически в то же время, что и модель Take-Grant, в 1976 году. Она используется преимущественно для анализа системы защиты, реализующей дискреционную политику безопасности, и ее основного элемента – матрицы доступов. При этом система представляется конечным автоматом, функционирующим согласно определенным правилам перехода.

Введем следующие обозначения: O – множество объектов системы; S – множество субъектов системы ($S \subseteq O$); R – множество прав доступа субъектов к объектам, например права на чтение, запись, владение; M – матрица доступа, строки которой соответствуют субъектам, а столбцы – объектам; $M[s, o] \subseteq R$ – права доступа субъекта s к объекту o.

Отдельный автомат, построенный согласно положениям модели HRU, будем называть системой. Функционирование системы рассматривается только с точки зрения изменений в матрице доступа. Возможные изменения определяются шестью примитивными операторами:

– «внести» право $r \in R$ в $M[s, o]$ – добавление субъекту s права доступа r к объекту o. При этом в ячейку M[s, o] матрицы доступов добавляется элемент r. Условия выполнения: $s \in S$, $o \in O$. Результат:

$$S' = S, O' = O, M'[s, o] = M[s, o] \cup \{r\},$$

$$(s', o') \neq (s, o) \Rightarrow M'[s', o'] = M[s', o];$$

– «удалить» право $r \in R$ из $M[s, o]$ – удаление у субъекта s права доступа r к объекту o. При этом из ячейки M[s, o] матрицы доступов удаляется элемент r. Условия выполнения: $s \in S$, $o \in O$. Результат:

$$S' = S, O' = O, M'[s, o] = M[s, o] \setminus \{r\},$$

$$(s', o') \neq (s, o) \Rightarrow M'[s', o'] = M[s', o'];$$

– «создать» субъект s' – добавление в систему нового субъекта s'. При этом в матрицу доступов добавляется новые столбец и строка. Условия выполнения: $s' \notin S$. Результат:

–

$$S' = S \cup \{s'\}, O' = O \cup \{s'\},$$

$$(s, o) \in SxO \Rightarrow M'[s, o] = M[s, o],$$

$$o \in O' \Rightarrow M'[s', o] = \varnothing, s \in S' \Rightarrow M'[s, s'] = \varnothing;$$

– «создать» объект o' – добавление в систему нового объекта o'. При этом в матрицу доступов добавляется новый столбец. Условия выполнения: $o' \notin O$. Результат:

$$S' = S, O' = O \cup \{o'\},$$

$$(s, o) \in SxO \Rightarrow M'[s, o] = M[s, o],$$

$$s \in S' \Rightarrow M'[s, o'] = \varnothing;$$

– «уничтожить» субъект s' – удаление из системы субъекта s'. При этом из матрицы доступов удаляются соответствующие столбец и строка. Условия выполнения: $s' \in S$. Результат:

$$S' = S / \{s'\}, O' = O / \{s'\},$$

$$(s, o) \in S'xO' \Rightarrow M'[s, o] = M[s, o];$$

– «уничтожить» объект o' – удаление из системы объекта o'. При этом из матрицы доступов удаляется соответствующий столбец. Условия выполнения: $o' \in O$, $o' \notin S$. Результат:

–

$$S' = S, O' = O / \{o'\},$$

$$(s, o) \in S'xO' \Rightarrow M'[s, o] = M[s, o].$$

Из примитивных операторов могут составляться команды, каждая из которых состоит из двух частей: условия, при котором выполняется команда, и последовательности примитивных операторов.

Как уже упоминалось выше, согласно требованиям большинства критериев оцени безопасности, системы защиты должны строиться на основе определенных математических моделей, с помощью которых должно быть теоретически обосновано соответствие системы защиты требованиям заданной политики безопасности. Для решения поставленной задачи необходим алгоритм, осуществляющий данную проверку. Однако, как показывают результаты анализа модели HRU, задача построения алгоритма проверки безопасности систем, реализующих дискреционную политику разграничения прав доступа, не может быть решена в общем случае. С одной стороны, общая модель HRU может выражать большое разнообразие политик дискреционного разграничения доступа, но при том не существует алгоритма проверки их безопасности. С другой стороны, можно использовать моно операционные системы, для которых алгоритм проверки безопасности существует, но данный класс систем является слишком узким. Например, моно операционные системы не могут выразить политику, дающую субъектам права на созданные ими объекты, так как не существует одной операции, которая и создает объект, и помечает его как принадлежащий создающему субъекту одновременно.

Еще одна классическая модель системы безопасности – **модель Bell-laPadula**, предназначенная для анализа систем защиты, реализующих мандатное (полномочное) разграничение доступа. Она также известна под названием «многоуровневая модель безопасности», а системы, ее реализующие – системы с многоуровневой безопасностью (multilevel secure systems, MLS). В данной модели определяется, какими свойствами должны обладать состояния и действия системы, чтобы она была безопасной, но не указывается, что должна делать система по запросам на доступ субъектов к объектам при переходе из состояния в состояние, и как именно должны при этом изменяться значения элементов модели.

Модель Low-Water-Mark (LWM) представляет близкий к модели Bell-laPadula подход к определению свойств системы безопасности, реализующей мандатную политику безопасности. В модели LWM предлагается порядок безопасного функционирования системы в случае, когда по запросу субъекта ему всегда необходимо предоставлять доступ на запись в объект.

Другими примерами моделей безопасности являются модель Biba, Clark-Wilson, модель «китайской стены», описанные в [5], и др.

Все рассмотренные модели могут быть использованы при построении и анализе детерминированных систем защиты, т. е. систем, которые не включают элементов, имеющих вероятностную природу. При исследовании систем, закономерности функционирования которых сложны или практически не поддаются описанию, целесообразно использовать элементы теории вероятностей. К числу таких систем относятся

глобальные вычислительные сети, современные многозадачные и многопользовательские операционные системы.

Методы удаленного администрирования автоматизированных систем используют распределенную вычислительную среду, и для их анализа рассмотренные модели безопасности в классическом виде неприменимы.

Одна из моделей, которую можно использовать для анализа безопасности распределенных систем, – модель безопасности информационных потоков.

В данной модели все объекты системы делятся на две непересекающиеся группы: высокоуровневые объекты, имеющие право обрабатывать информацию высокого уровня секретности, и низкоуровневые. Все взаимодействия между данными группами объектов осуществляются через систему защиты.

На множестве объектов системы задается вероятностное распределение, оба множества состояний объектов являются случайными величинами. Для описания и анализа информационных потоков между ними используются понятия независимости и условного распределения. Данная модель рассматривает два подхода к определению безопасности информационных потоков, основанных на понятиях информационной невыводимости и информационного невмешательства.

Модель безопасности информационных потоков служит практическим примером подхода к построению системы защиты, которая разрешает корреляцию значений высокоуровневых и низкоуровневых объектов, но при этом остается безопасной.

С точки зрения методов удаленного администрирования, основанных на технологии «клиент-сервер», множество высокоуровневых объектов находится на серверной части, а низкоуровневых – на удаленных клиентских станциях, которые принимают управляющие команды, обрабатывают их и возвращают результат обработки серверу. Но с другой стороны, если абстрагироваться до уровня клиентской части, то множество высокоуровневых объектов представляет собой набор компонентов программы удаленного администрирования, например, специальной службы, драйвера и динамических модулей, а множество низкоуровневых объектов – пользовательские файлы. Поэтому необходимо также учитывать локальную политику безопасности для каждой клиентской станции.

В результате, можно сделать вывод, что для исследования и анализа безопасности систем, использующих в своей работе методы удаленного доступа и администрирования, не подходит ни одна из классических формальных моделей безопасности. Для получения наиболее точной оценки эффективности защиты таких систем необходимо использовать сочетание моделей, предназначенных для исследования детерминированных систем защиты, и моделей для анализа безопасности информационных потоков в распределенной вычислительной среде. Другой подход – разработка новой специализированной модели, учитывающей факторы удаленного администрирования автоматизированных систем, является темой дальнейших исследований в данной области.

Литература: 1. НД ТЗИ 1.1-003-99. Терминология в области защиты информации в компьютерных системах от несанкционированного доступа. // Департамент специальных телекоммуникационных систем и защиты информации Службы безопасности Украины. - Киев, 1999. 2. Проскурин В. Г. и др. Защита в операционных системах. – М., 2000. 3. Девянин П. Н. и др. Теоретические основы компьютерной безопасности. – М., 2000. 4. Michael A. Harrison. Theoretical Issues Concerning Protection in Operating Systems. 5. Ross J. Anderson. Lectures on Computer Science – Security. University of Cambridge, 1999.

УДК 638.235.231

ПРО ОДИН ПІДХІД ДО ВИЗНАЧЕННЯ ПОТРЕБ КОРПОРАТИВНИХ КОМП'ЮТЕРНИХ МЕРЕЖ ЩОДО ЗАХИСТУ ІНФОРМАЦІЇ

Антон Михайлюк, Сергій Гончарук, Сергій Колотило
Національний Технічний Університет України «КПІ"

Анотація: **Розроблено механізм визначення потреб у захисті багаторівневих неоднорідних інформаційно-обчислювальних систем і побудови на основі отриманих даних комплексного засобу захисту, що відповідає державним стандартам технічного захисту інформації від несанкціонованого доступу.**